

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
BRYAN COHEN, individually and on behalf of :
all other persons similarly situated, :
Plaintiff, :
:
v. :
:
NORTHEAST RADIOLOGY, P.C. and :
ALLIANCE HEALTHCARE SERVICES, INC., :
Defendants. :
-----X

OPINION AND ORDER

20 CV 1202 (VB)

Briccetti, J.:

Plaintiff Bryan Cohen brings this putative class action against defendants Northeast Radiology, P.C. (“Northeast Radiology”), and Alliance Healthcare Services, Inc. (“Alliance”), for violations of state law.

Now pending are defendants’ motion to dismiss the first amended complaint (“FAC”) for lack of subject matter jurisdiction, Fed. R. Civ. P. 12(b)(1), and for failure to state a claim, Fed. R. Civ. P. 12(b)(6) (Doc. #35); plaintiff’s motion to appoint interim lead class counsel (Doc. #22); and plaintiff’s motion for an order pursuant to Rule 23(d) (Doc. #51).

For the following reasons, the motion to dismiss is GRANTED IN PART and DENIED IN PART, the motion to appoint interim lead class counsel is DENIED, and the motion for an order pursuant to Rule 23(d) is DENIED.

BACKGROUND

For the purpose of ruling on the motions, the Court accepts as true all well-pleaded allegations in the FAC and draws all reasonable inferences in plaintiff’s favor, as summarized below. The Court also considers the March 10, 2020, letter sent by

Northeast Radiology to plaintiff (“March 10 Letter”), and Northeast Radiology’s March 11, 2020, Press Release (“Press Release”) as incorporated by referenced into the FAC.¹

Plaintiff alleges that as a patient of Northeast Radiology in December 2016, he provided them with his name, address, and social security number (“SSN”), which, in addition to other information associated with his treatment, were stored on defendants’ servers. According to plaintiff, unauthorized individuals accessed this information during a data breach of defendants’ servers between April 14, 2019, and January 7, 2020, (the “Breach Period”), causing plaintiff various harms, including identity theft.

Plaintiff claims that on January 10, 2020, TechCrunch, an online newspaper, published an article that independent cybersecurity researchers from Greenbone Networks (“Greenbone”) had announced they had uncovered major flaws in defendants’ systems that permitted unauthorized access to more than 1.2 million patients’ medical records. According to plaintiff, a month before these results were published, Greenbone notified defendants of the data breach, but defendants continued to operate systems that allowed the unauthorized parties to access patient information. According to plaintiff, it was only after TechCrunch reporters questioned defendants about the Greenbone findings that defendants made changes to their systems to reduce the risk of unauthorized access.

¹ Both of these documents are referenced in the FAC but not attached to the FAC. Accordingly, the Court incorporates by reference the March 10 Letter (Doc. #35-3) and the Press Release (Doc. #35-4) defendants submitted with their motion to dismiss. A court assessing a Rule 12(b)(6) motion may “consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint.” DiFolco v. MSNBC Cable L.L.C., 622 F.3d 104, 111 (2d Cir. 2010).

Unless otherwise indicated, case quotations omit all internal citations, quotation marks, footnotes, and alterations.

On March 11, 2020, Northeast Radiology issued the Press Release which stated that unauthorized individuals had gained access to Northeast Radiology's picture archiving and communication system ("PACS"). The PACS stored electronic protected health information ("e-PHI"), specifically, radiology images and related information, including name, gender, age, date of birth, exam description, date of service, image, image description, and medical record number, which in some instances, could correspond to the patient's SSN. The Press Release stated that defendants had conducted an internal investigation, which revealed that twenty-nine patients' e-PHI was accessed during the breach. It also stated that Northeast Radiology was notifying the twenty-nine patients that their e-PHI had been revealed, and that patients whose information was stored on the system—but was not confirmed as being accessed by unauthorized users (the "other patients")—were also being notified. Plaintiff alleges that as one of the "other patients," he received such a letter dated March 10, 2020 (i.e., the March 10 Letter).

Plaintiff alleges he was harmed by the data breach. He claims that a lender contacted him in September 2019 regarding a fraudulent loan application made using his name, address, and SSN. He also alleges that more than \$10,000 in unreimbursed fraudulent charges were made to his bank account during the Breach Period. According to plaintiff, these events caused his credit score to drop from 730 to 466, which resulted in the denial of his application for an apartment rental. Plaintiff also alleges he has spent many hours "dealing with credit agencies to 'lock' his file," contacting financial institutions to inform them of fraud and to prevent future attacks, closing bank accounts, and closely monitoring credit reports and accounts for unauthorized activity. (FAC ¶ 8).

In addition, plaintiff alleges that a result of defendants' data breach, he remains at risk of further identity theft, including that his e-PHI can be used for unauthorized withdrawals from his bank account; to obtain identification documents, government benefits, a house rental, or medical services in his name; to file fraudulent tax returns in his name; or to provide plaintiff's name in a police arrest. He also alleges he will be required to purchase credit and identity theft monitoring services and expend additional time and effort to prevent and mitigate potential future losses.

DISCUSSION

I. Standards of Review

A. Rule 12(b)(1)

"[F]ederal courts are courts of limited jurisdiction and lack the power to disregard such limits as have been imposed by the Constitution or Congress." Durant, Nichols, Houston, Hodgson & Cortese-Costa, P.C. v. Dupont, 565 F.3d 56, 62 (2d Cir. 2009). "A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it." Nike, Inc. v. Already, LLC, 663 F.3d 89, 94 (2d Cir. 2011). A court lacks the judicial power to hear a party's claims when the party does not have standing. Hillside Metro Assocs., LLC v. JPMorgan Chase Bank, Nat'l Ass'n, 747 F.3d 44, 48 (2d Cir. 2014).

When deciding whether subject matter jurisdiction exists at the pleading stage, the court "must accept as true all material facts alleged in the complaint." Conyers v. Rossides, 558 F.3d 137, 143 (2d Cir. 2009). "However, argumentative inferences

favorable to the party asserting jurisdiction should not be drawn.” Buday v. N.Y. Yankees P’ship, 486 F. App’x 894, 895 (2d Cir. 2012) (summary order).

When a defendant moves to dismiss for lack of subject matter jurisdiction and on other grounds, the court should resolve the Rule 12(b)(1) challenge first. Rhulen Agency, Inc. v. Ala. Ins. Guar. Ass’n, 896 F.2d 674, 678 (2d Cir. 1990).

B. Rule 12(b)(6)

In deciding a Rule 12(b)(6) motion, the Court evaluates the sufficiency of the operative complaint under the “two-pronged approach” articulated by the Supreme Court in Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009). First, plaintiff’s legal conclusions and “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements,” are not entitled to the assumption of truth and are thus not sufficient to withstand a motion to dismiss. Id. at 678; Hayden v. Paterson, 594 F.3d 150, 161 (2d Cir. 2010). Second, “[w]hen there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief.” Ashcroft v. Iqbal, 556 U.S. at 679.

To survive a Rule 12(b)(6) motion, the allegations in the complaint must meet a standard of “plausibility.” Ashcroft v. Iqbal, 556 U.S. at 678; Bell Atl. Corp. v. Twombly, 550 U.S. 544, 564 (2007). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 556 U.S. at 678. “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” Id. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. at 556).

II. Jurisdiction Under the Class Action Fairness Act (“CAFA”)

Defendants argue the Court lacks subject matter jurisdiction under CAFA because plaintiff has not plausibly alleged the requisite amount-in-controversy or that the proposed class is equal to or greater than 100 individuals.

The Court disagrees.

CAFA grants federal jurisdiction over certain class actions in which at least \$5,000,000 is in controversy, the class exceeds 100 individuals, and the parties are minimally diverse. 28 U.S.C. § 1332(d).

“Under CAFA, as under the traditional rule, the party asserting subject matter jurisdiction has the burden of proving it.” Blockbuster, Inc. v. Galeno, 472 F.3d 53, 59 (2d Cir. 2006). As to the amount-in-controversy, the movant “must show that it appears to a ‘reasonable probability’ that the aggregate claims of the plaintiff class are in excess of \$5 million.” Id. at 58.

“In satisfying the ‘reasonable probability’ burden, there is a rebuttable presumption that the face of the complaint is a good faith representation of the actual amount in controversy.” See Shulman v. Chaitman LLP, 392 F. Supp. 3d 340, 354 (S.D.N.Y. 2019). “To overcome the face-of-the complaint presumption, the party opposing jurisdiction must show ‘to a legal certainty’ that the amount recoverable does not meet the jurisdictional threshold.” Id. “[T]he legal impossibility of recovery must be so certain as virtually to negate the plaintiff’s good faith in asserting the claim. If the right of recovery is uncertain, the doubt should be resolved in favor of the subjective good faith of the plaintiff.” Chase Manhattan Bank, N.A. v. Am. Nat. Bank & Tr. Co. of Chicago, 93 F.3d 1064, 1070 (2d Cir. 1996).

Here, plaintiff adequately alleges the Court's subject matter jurisdiction under CAFA.

Plaintiff alleges that he has personally sustained more than \$10,000 in fraudulent charges as a result of the data breach. He also alleges that defendants housed over 1.2 million individuals' e-PHI on their servers and that the servers were accessed by unauthorized individuals for almost nine months. At this early stage, these allegations plausibly plead a "reasonable probability" that the aggregate claims are in excess of \$5 million.

In addition, defendants have failed to satisfy the "legal certainty" threshold required to overcome the presumption of good faith accorded to plaintiff's allegations regarding the amount-in-controversy. Defendants' argument that they are "not aware of any more than twenty-nine individuals whose records were accessed" and that "one cannot extrapolate every putative class member has the monetary loss Plaintiff alleges" falls short of showing to a "legal certainty" that the putative class cannot recover the amount claimed. (Defs. Reply at ECF 12).² Indeed, by defendants' own admission, there may be other patients beyond the twenty-nine definitively-identified patients whose information was accessed: the Press Release states defendants "do not have evidence about whose particular information may have been accessed, if at all." (Doc. #35-4). Moreover, the March 10 Letter offers to patients a complimentary year-long membership in a program that helps detect possible misuse of personal information and provides identity theft protection services. These statements suggest not a "legal impossibility of

² "ECF __" refers to page numbers automatically assigned by the Court's Electronic Case Filing system.

recovery,” but rather that a possibility of recovery exists. Chase Manhattan Bank, N.A. v. Am. Nat. Bank & Tr. Co. of Chicago, 93 F.3d at 1070.

Finally, given the early stage of the proceedings, plaintiff’s allegation that more than 1.2 million patients’ information was stored on defendants’ servers suffices to allege the class exceeds 100 members.

Accordingly, defendants’ motion to dismiss for lack of subject matter jurisdiction under CAFA must be denied.

III. Standing

Defendants argue plaintiff does not have standing to bring this action.

The Court disagrees.

A. Legal Standard

To satisfy the “irreducible constitutional minimum of standing . . . the plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). When, as here, “the Rule 12(b)(1) motion is facial, i.e., based solely on the allegations of the complaint or the complaint and exhibits attached to it . . . , the plaintiff has no evidentiary burden.” John v. Whole Foods Mkt. Grp., Inc., 858 F.3d 732, 736 (2d Cir. 2017). “The task of the district court is to determine whether the [complaint] alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue.” Id.

B. Injury-in-Fact

1. Applicable Law

An injury-in-fact is “an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” Spokeo, Inc. v. Robins, 136 S. Ct. at 1548. “For an injury to be particularized, it must affect the plaintiff in a personal and individual way,” and in order to be “concrete,” the injury “must actually exist.” Id. The Second Circuit has “repeatedly described [the injury-in-fact] requirement as a low threshold which helps to ensure that the plaintiff has a personal stake in the outcome of the controversy.” John v. Whole Foods Mkt. Grp., Inc., 858 F.3d at 736. “Any monetary loss suffered by the plaintiff satisfies [the injury-in-fact] element; even a small financial loss suffices.” Carter v. HealthPort Techs., LLC, 822 F.3d 47, 55 (2d Cir. 2016). Time and expense to respond to a data breach, may also satisfy the injury-in-fact requirement. See Rudolph v. Hudson’s Bay Co., 2019 WL 2023713, at *6–7 (S.D.N.Y. May 7, 2019).

In addition, “[a] plaintiff has Article III standing if she plausibly alleges future injury, provided that ‘the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.’” Rudolph v. Hudson’s Bay Co., 2019 WL 2023713, at *3 (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)). Indeed, “[a]n injury may include mitigation-related expenses ‘based on a substantial risk that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.’” Id. (quoting Clapper v. Amnesty Intern. USA, 568 U.S. 398, 415 n.5 (2013)).

Still, “[a]lthough Supreme Court precedent does not ‘uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about’—

hence, the ‘substantial risk’ standard—no Article III standing exists if a plaintiff’s theory of injury rests on an ‘attenuated chain of inferences necessary to find harm.’” Steven v. Carlos Lopez & Assocs., LLC, 422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019) (quoting Clapper v. Amnesty Intern. USA, 568 U.S. at 415 n.5). Moreover, a “subjective fear” or “speculative threat” is not enough to identify injury. Clapper v. Amnesty Intern. USA, 568 U.S. at 416.

“Applying these principles, many courts have held that plaintiffs alleging the theft of personal identifying information in a data breach have standing to bring claims against the entity that had held their data based on an increased risk of future identity theft.” Steven v. Carlos Lopez & Assocs., LLC, 422 F. Supp. 3d at 804 (collecting cases). In such cases, “the data was stolen by hackers or cyber criminals who had intentionally targeted the data.” Id. at 805 (analyzing collected cases). The “intentional act of theft gave rise, in turn, to a plausible inference that the stolen data would be misused.” Id. Indeed, “[i]n several of these cases, at least one named plaintiff alleged actual misuse of his or her personal information by the suspected data thief.” Id. at 804. However, absent an allegation that an unauthorized third party intentionally stole the data, “courts have concluded that the risk of identity theft is too speculative to support Article III standing.” Id. at 805 (collecting cases).

2. Application

Plaintiff alleges six injuries as a consequence of the data breach: (i) in September 2019, a lender contacted him regarding a fraudulent loan application made using his name, address, and SSN, (ii) more than \$10,000 in unreimbursed fraudulent charges made to his bank account during the Breach Period, (iii) a drop in his credit score, leading

to a denial of apartment rental, (iv) hours spent communicating with credit agencies and financial institutions and monitoring credit reports and accounts, (v) the remaining risk of future identity theft, and (vi) that he will be required to purchase credit and identity theft monitoring services and expend additional time and effort to prevent and mitigate potential future losses.

At a minimum, plaintiff's allegation that he was not reimbursed for \$10,000 in fraudulent charges made to his bank account satisfies the injury-in-fact requirement. See Carter v. HealthPort Techs., LLC, 822 F.3d at 55. Plaintiff's additional allegation that he has spent time communicating with credit agencies and financial institutions and monitoring credit reports and accounts further supports the contention that plaintiff has suffered an injury-in-fact. See Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *1 ("[T]he time and expense that [plaintiff] expended in order to obtain a replacement debit card are sufficient to satisfy the 'low threshold' required to allege injury-in-fact and demonstrate Article III standing.").

Moreover, plaintiff alleges both that the information stored on defendants' servers was stolen intentionally and "actual misuse of his or her personal information by the suspected data thief." See Steven v. Carlos Lopez & Assocs., LLC, 422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019); id. at 805 ("[The] intentional act of theft gave rise, in turn, to a plausible inference that the stolen data would be misused."). Indeed, plaintiff alleged that during the Breach Period, he was contacted about a fraudulent loan in his name and that \$10,000 fraudulent charges were made to his bank account. Accordingly, the alleged risk of future identity theft is not too speculative to support Article III standing.

C. Fairly Traceable

“The causal connection element of Article III standing, i.e., the requirement that the plaintiff’s injury be fairly traceable to the challenged action of the defendant . . . does not create an onerous standard. For example, it is a standard lower than that of proximate causation.” Carter v. HealthPort Techs., LLC, 822 F.3d at 55.

Here, plaintiff alleges that as a patient of Northeast Radiology, he provided defendants with his name, address, and SSN, which, along with other e-PHI associated with his treatment, were stored on defendants’ servers; that from April 14, 2019, to January 7, 2020, (i.e., the Breach Period), unauthorized individuals accessed e-PHI stored on defendants’ servers; and that during the Breach Period, plaintiff was contacted by a lender regarding a fraudulent loan application and he experienced fraudulent charges to his bank account totaling more than \$10,000. Thus, plaintiff plausibly alleges his harm is fairly traceable to defendants’ failure to prevent the data breach. See Lewert v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963, 965, 969 (7th Cir. 2016) (allegedly fraudulent charges incurred two months after plaintiff dined at national restaurant chain had suffered data breach fairly traceable to that breach absent allegation that the location plaintiff visited was hacked).

Plaintiff also alleges that the Press Release states defendants had determined twenty-nine patients’ information was accessed in the data breach. The Press Release also states defendants were unable to determine which other patients’ information, if any, was accessed but that nevertheless, they had informed the other patients of the data breach. This suggests defendants considered the risk to the other patients, including plaintiff, significant enough to send a letter warning of the potential e-PHI exposure. Cf.

Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d at 968 (“When the data system for an entire corporation with locations across the country experiences a data breach and the corporation reacts as if that breach could affect all of its locations, it is certainly plausible that all of its locations were in fact affected.”).³

Furthermore, defendants’ argument that plaintiff fails plausibly to allege traceability because other data breaches may have exposed his personal information has no bearing on plaintiff’s standing to sue. See Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 757 (W.D.N.Y. 2017) (collecting cases) (“[C]ourts have rejected the argument that plaintiffs’ injuries are not fairly traceable when their information could have been compromised during a different data breach in recent years.”). Defendants may raise such a challenge as a defense at a later stage in the litigation. Id. at 757–58.

For the reasons above, plaintiff plausibly alleges he has standing to pursue his claims, and defendants’ motion to dismiss for lack of standing must be denied.⁴

IV. Failure to State A Claim

Defendants argue plaintiff’s causes of action for (i) negligence, (ii) negligence per se, (iii) breach of contract, (iv) breach of implied contract, and (v) violations of General Business Law (“G.B.L.”) § 349 should all be dismissed.

³ Defendants’ argument that plaintiff’s information may not have actually been exposed in the data breach identifies a factual dispute about the scope of the data breach, but it does not destroy standing. At summary judgment, or at trial, defendants may present evidence to explain how the breach occurred and which patients’ information was accessed. See Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d at 968.

⁴ Defendants raised no argument regarding redressability.

The Court agrees as to the negligence per se and breach of contract claims, but disagrees as to the claims for negligence, implied breach of contract, and violation of Section 349.

A. Negligence

Defendants argue plaintiff fails to allege proximate cause and damages as to the negligence claim.

The Court disagrees.

Under New York law, to plead a negligence claim, a plaintiff must plausibly allege “(1) the defendant owed the plaintiff a cognizable duty of care; (2) the defendant breached that duty; and (3) the plaintiff suffered damage as a proximate result of that breach.” Stagl v. Delta Airlines, Inc., 52 F.3d 463, 467 (2d Cir. 1995).

Regarding proximate cause, plaintiff alleges that his e-PHI was stored on defendants’ PACS server; defendants failed to take adequate measures to protect the e-PHI, resulting in the data breach; and plaintiff’s e-PHI was compromised, resulting in fraudulent loans and charges made in his name during the Breach Period. At this stage of the case, this sufficiently alleges defendants’ conduct was the proximate cause of plaintiff’s injuries.

Regarding damages, plaintiff alleges he was not reimbursed for \$10,000 in fraudulent charges to his bank account and that he spent hours communicating with credit agencies and financial institutions and monitoring credit reports and accounts. These allegations sufficiently allege damages. See Rudolph v. Hudson’s Bay Co., 2019 WL 2023713, at *9 (plaintiff “identified loss based on the expense she incurred when she

drove to a Bank of America branch to obtain a new debit card, as well as time expended to retrieve the card and update account records”).

Defendant’s argument that plaintiff has not pleaded proximate cause because plaintiff does not allege his specific data was accessed is “more appropriately addressed at summary judgment or at trial.” See Rudolph v. Hudson’s Bay Co., 2019 WL 2023713, at *9. Moreover, defendant is wrong that the economic loss doctrine bars plaintiff’s negligence claim. See id. (declining to apply economic loss rule in data breach case); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (same).

Accordingly, plaintiff’s negligence claim may proceed.

B. Negligence Per Se

Defendants argue plaintiff has not pleaded a negligence per se claim.

The Court agrees.

Under the rule of negligence per se, if (1) a statute is designed to protect a class of persons, (2) in which the plaintiff is included, (3) from the type of harm which in fact occurred as a result of its violation, the issues of the defendant’s duty of care to the plaintiff and the defendant’s breach of that duty are conclusively established upon proof that the statute was violated.

Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d at 748.

“The issue of whether a plaintiff can assert a cause of action based on negligence per se is closely related to the question of whether a private cause of action exists under a statute.” Dubai Islamic Bank v. Citibank, N.A., 126 F. Supp. 2d 659, 668 (S.D.N.Y. 2000). Where the statute “does not express a private right of action . . . the existence of a private right of action turns upon whether it fairly can be implied from a reading of the statute.” Id. “In making this determination, the Court examines the following factors: (1) whether the plaintiff is a member of a class for whose special benefit the statute was

enacted, (2) whether there is any indication of legislative intent to create or deny a private right, (3) whether it would be consistent with the purposes of the underlying statutory scheme to create a private right, and (4) whether the cause of action is one traditionally relegated to state law.” Id.

Neither the Health Insurance Portability and Accountability Act (“HIPAA”) nor the Federal Trade Commission Act (“the FTC Act”) provide for an express private right of action. See Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d at 777. Indeed, that neither statutory scheme creates a private right of action weighs heavily against implying a private right of action necessary to sustain a negligence per se claim based upon either HIPAA or the FTC Act. Moreover, neither the parties nor the Court have identified a single case in this Circuit that has recognized that a private cause of action for negligence per se arises under New York law from violations of HIPAA or the FTC Act. And several New York courts have concluded that neither HIPAA nor the FTC Act can sustain a negligence per se claim. See Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 69 Misc. 3d 597, 608 (Sup. Ct. Westchester Cty. 2020) (“Plaintiff’s negligence per se claim based on an alleged violation of the FTC Act must also be dismissed because if mere proof of a violation of were to establish negligence per se, plaintiff would effectively be afforded a private right of action that the statute does not recognize.”); Abdale v. N. Shore Long Island Jewish Health Sys., Inc., 49 Misc. 3d 1027, 1038 (Sup. Ct. Queens Cty. 2015) (dismissing negligence per se claim because “HIPAA and its regulations do not create a private right of action”).

Accordingly, plaintiff’s negligence per se claim must be dismissed.

C. Breach of Contract

Defendants argue Northeast’s Notice of Privacy Practices does not form a contract.

The Court agrees.

“Under New York law, a breach of contract claim requires proof of (1) an agreement, (2) adequate performance by the plaintiff, (3) breach by the defendant, and (4) damages.” Fischer & Mandell LLP v. Citibank, N.A., 632 F.3d 793, 799 (2d Cir. 2011).

“An agreement stems from a manifestation of mutual assent sufficiently definite to assure that the parties are truly in agreement with respect to all material terms.” McCabe v. ConAgra Foods, Inc., 681 F. App’x 82, 84 (2d Cir. 2017) (summary order). “An agreement generally requires an offer and an acceptance.” Id.

Here, plaintiff fails plausibly to allege there was an agreement between plaintiff and defendants. According to plaintiff, Northeast Radiology’s Notice of Privacy Practices, available on its website, expressly promised to safeguard plaintiff’s e-PHI in accordance with applicable state and federal law. He further alleges he entered into a contract with defendants when he provided his e-PHI to defendants as “part of a transaction in which [he] paid money for radiological and/or medical goods and services.” (FAC ¶ 122). However, beyond stating in conclusory fashion that the parties entered into a contract, plaintiff offers no plausible allegations to support the conclusion that the parties had a contractual relationship. See Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d at 750 (dismissing breach of express contract claim when complaint “fails to allege any facts to support the conclusion that Defendant expressly contracted to protect employees’ PII [personally identifiable information]”). Indeed, the FAC does not describe any express agreement entered into by the parties. Nor does it attach or quote

any contract. “By failing to allege any facts upon which a finding of express contract regarding PII could be predicated, the Complaint engages in the type of ‘[t]hreadbare recital[] of the elements of a cause of action’ that Iqbal warned against.” Id. (quoting Ashcroft v. Iqbal, 556 U.S. at 678).⁵

Accordingly, plaintiff’s claim for breach of contract must be dismissed.

D. Breach of Implied Contract

Defendants also argue plaintiff fails to state a claim for breach of implied contract.

The Court disagrees.

“Under New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct.” Leibowitz v. Cornell Univ., 584 F.3d 487, 506–07 (2d Cir. 2009). An implied contract, like an express contract, requires “consideration, mutual assent, legal capacity and legal subject matter.” Id. at 507.

Here, “[p]laintiff[] allege[s] conduct and a course of dealing that raise[s] a strong inference of implied contract.” Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d at 750. Plaintiff alleges that defendants obtained, created, and maintained e-PHI as part of providing radiological services to their patients, evincing an implicit promise by defendants to protect their patients’ e-PHI from unauthorized users. Indeed, plaintiff’s

⁵ The two cases plaintiff cites for the proposition that writings such a privacy policy may be considered “the basis of the contract,” see Pl. Br. at ECF 26 (citing Miller v. Mercuria, 291 F. Supp. 3d 509, 518 (S.D.N.Y. 2018), and Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d at 761), are inapposite, because here there is no separate, other contract into which the Notice of Privacy Practices can be incorporated.

allegations that defendants' Notice of Privacy Practices outlines the limited circumstances under which patient e-PHI would be disclosed—none of which included granting access to unauthorized third parties—“further supports a finding of an implicit promise” that defendants would safeguard patients' e-PHI. See id. Plaintiff also plausibly alleges he accepted the offer by becoming a patient at the facility, providing his e-PHI, and paying for defendants' services, and that by failing to safeguard his e-PHI and timely informing him of the breach, defendants breached the implied contract. And, as discussed, plaintiff has sufficiently alleged damages. See supra Part IV.A.

Accordingly, plaintiff's breach of implied contract claim may proceed.

E. Deceptive Trade Practices

Defendants argue plaintiff fails to state a claim under G.B.L. § 349 because plaintiff has not alleged causation or injury.

The Court disagrees.

Section 349 prohibits “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service.” N.Y. Gen. Bus. § 349(a). To successfully assert a Section 349 claim, “a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice.” Orlander v. Staples, Inc., 802 F.3d 289, 300 (2d Cir. 2015). New York courts define the term “deceptive acts and practices” objectively, as “representations or omissions, limited to those likely to mislead a reasonable consumer acting reasonably under the circumstances.” Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A., 85 N.Y.2d 20, 26 (1995). Claims based on omissions are cognizable “where the

business alone possesses material information that is relevant to the consumer and fails to provide this information.” Id.

Here, plaintiff alleges defendants misrepresented that they would adequately protect plaintiff’s e-PHI and that they did not inform of him of the breach within 60 days, in violation of the Notice of Privacy Practices. Based on these allegations, “it is at least plausible that [defendants’] representations in their [Notice of Privacy Practices] concerning data security [] would lead a reasonable consumer to believe that [defendants] were providing more adequate data security than they purportedly were.” Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d at 776. “It is also at least plausible that [defendants’] failure to disclose the purportedly inadequate data security measures would mislead a reasonable consumer.” Id. And, as discussed, plaintiff has sufficiently alleged damages. See supra Part IV.A.

Accordingly, plaintiff’s Section 349 claim may proceed.

V. Appointment of Interim Lead Class Counsel

Plaintiff argues Lowey Dannenburg P.C. should be appointed interim lead class counsel.

The Court disagrees.

When a Court certifies a class, it must appoint class counsel. Fed R. Civ. P. 23(g)(1). However, “[t]he court may designate interim counsel to act on behalf of a putative class before determining whether to certify the action as a class action,” Fed R. Civ. P. 23(g)(3) (emphasis added), if such designation is “necessary to protect the interests of the putative class.” Fed. R. Civ. P. 23 advisory committee’s note to 2003 amendment.

Ordinarily, the lawyer who files the action handles precertification matters such as preparing for the certification decision, making and responding to motions, and discussing settlement. See Fed. R. Civ. P. 23 advisory committee’s note to 2003 amendment. However, in some instances, “rivalry or uncertainty [may] make[] formal designation of interim counsel appropriate.” Id.

“Generally, courts will appoint interim class counsel only in the event that there are a number of overlapping, duplicative, or competing suits pending in other courts, and some or all of those suits may be consolidated, with multiple attorneys vying for class counsel appointment.” Sullivan v. Barclays PLC, 2013 WL 2933480, at *1 (S.D.N.Y. June 11, 2013) (citing Federal Judicial Center, Manual for Complex Litigation § 21.11 (4th ed. 2004)). Indeed, “[i]f the lawyer who filed the suit is likely to be the only lawyer seeking appointment as class counsel, appointing interim class counsel may be unnecessary.” Federal Judicial Center, Manual for Complex Litigation § 21.11.

Here, “movants have not come forward with any showing as to why their appointment as interim class counsel would be beneficial or necessary.” Sullivan v. Barclays PLC, 2013 WL 2933480, at *1. Plaintiff has identified neither any overlapping, duplicative, or competing lawsuit that may be consolidated with the instant action nor any competing counsel that may complicate efficient case management or complete duplicative work. See id.

Moreover, a lack of designation will neither harm the interests of the putative class nor inhibit Lowey Dannenburg’s ability to represent them going forward. “Whether or not formally designated interim counsel, an attorney who acts on behalf of the class

before certification must act in the best interests of the class as a whole.” Fed. R. Civ. P. 23 advisory committee’s note to 2003 amendment.

Plaintiff’s argument that there exists a risk of class members initiating proceedings in the future, leading to duplicative filings, is unpersuasive. The inquiry is whether the appointment of interim counsel is necessary, and the risk of future claims does not warrant appointment of interim counsel. Indeed, a premature appointment could “preemptively limit a full airing and evaluation of the appointment of class counsel, in the event that additional, overlapping actions do, in fact, materialize in the future.” Sullivan v. Barclays, 2013 WL 2933480, at *1.

The cases plaintiff’s counsel cites for the proposition that courts in this district grant motions to appoint interim lead class counsel where this is only one law firm applying for leadership are inapposite. For instance, in Bernstein v. Cengage Learning, Inc., two similar recent cases had been filed, leading the Court to conclude the “possibility of more such cases is not foreclosed.” 2019 WL 6324276, at *2 (S.D.N.Y. Nov. 26, 2019). And in In re JPMorgan Precious Metals Spoofing Litig., 18 Civ. 10356, Doc. #18 (S.D.N.Y. Feb. 5, 2019), and In re Mexican Gov’t Bonds Antitrust Litig., 18 Civ. 2830, Doc. #49 (S.D.N.Y. June 18, 2018), multiple cases had been filed by multiple plaintiff’s attorneys when the court consolidated the cases and appointed interim lead counsel.

Accordingly, plaintiff’s motion to appoint interim lead class counsel is denied.

VI. Rule 23(d) Corrective Notice

Plaintiff also moves for an order requiring “corrective notice” to putative class members and prohibiting further communications by defendants with putative class members absent leave of court.

The Court declines to issue such an order.

A. Legal Standard

Rule 23(d) authorizes courts, inter alia, to (1) require that appropriate notice be given to class members at “any step in the action” in order to “protect class members and fairly conduct the action”; (2) “impose conditions on the representative parties or on intervenors”; or (3) “deal with similar procedural matters.” Fed. R. Civ. P. 23(d)(1)(B)(i), (C), (E).

“Courts use Rule 23(d) to limit communications to protect class members from misleading communications from the parties or their counsel, because misleading communications to class members concerning the litigation pose a serious threat to the fairness of the litigation process, the adequacy of representation and the administration of justice generally.” Dodona I, LLC v. Goldman, Sachs & Co., 300 F.R.D. 182, 184 (S.D.N.Y. 2014). “The Court’s authority to regulate communications under Rule 23(d) also extends to communications that interfere with the proper administration of a class action, those that abuse the rights of members of the class, and situations in which there is a relationship that is inherently coercive.” Id.

“[A]n order limiting communications between parties and potential class members should be based on a clear record and specific findings that reflect a weighing of the need for a limitation and the potential interference with the rights of the parties.”

Gulf Oil Co. v. Bernard, 452 U.S. 89, 101 (1981).⁶ The Court’s discretion to enter such an order “is not unlimited, and indeed is bounded by the relevant provisions of the Federal Rules,” as well as by the First Amendment. See Gulf Oil Co. v. Bernard, 452 U.S. at 100. It “should result in a carefully drawn order that limits speech as little as possible, consistent with the rights of the parties under the circumstances.” Id. at 102. The Court’s supervisory authority under Rule 23(d) to limit communications exists even prior to class certification. See Urtubia v. B.A. Victory Corp., 857 F. Supp. 2d 476, 484 (S.D.N.Y. 2012).

B. Application

Plaintiff identifies two issues with defendants’ statements in the March 10 Letter to their patients regarding the data breach. First, plaintiff maintain defendants could not state in the March 10 Letter that they had “no reason to believe that any of [the recipient’s] personal information has been misused for the purpose of committing fraud or identity theft” because defendants do not have access to each individual’s financial records, such as bank records, that would confirm such a statement. (Doc. #35-3). Second, plaintiff argues the March 10 Letter’s statement that defendants “have no evidence that anyone viewed or acquired your specific personal information,” (id.) “directly contradicts” (Doc. #52 at ECF 7) the March 11 Press Release statement that defendants “do not have evidence about whose particular information may have been accessed, if at all” (Doc. # 35-4). According to plaintiff, these statements have misled

⁶ Although Gulf Oil v. Bernard concerned the plaintiffs’ communications with putative class members, courts have extended the reasoning to cover defendants’ communications with putative class members. See Dodona I, LLC v. Goldman, Sachs & Co., 300 F.R.D. at 185 (collecting cases).

putative class members into believing they have not suffered an injury from the data breach and do not need to take action to protect themselves from risk of future harm.

The Court is not persuaded that either of these statements are misleading. First, defendants' lack of access to each individual patient's financial records does not necessarily render false their statement that they had "no reason to believe that any of [the recipient's] personal information has been misused for the purpose of committing fraud or identity theft." Moreover, the March 10 Letter also relays defendants' offer of a complimentary year-long membership in a program that helps detect possible misuse of personal information and provides identity protection services. Thus, the Court concludes the March 10 Letter taken as a whole does not mislead putative class members into believing they have not suffered an injury and should not take action to prevent identity theft or fraud. Rather, the letter encourages recipients to monitor their records to ensure they are not harmed by any potential unauthorized access to their records.

Second, the Press Release states that other than the twenty-nine patients whose information was definitely accessed, defendants do not have evidence about whose information was accessed—if any other patient's information was accessed at all. That is not inconsistent with the March 10 Letter telling recipients that defendants did not have evidence that anyone viewed or accessed their information. Indeed, beyond conclusorily stating that these two statements are "directly contradict[ory]," plaintiff offers no explanation of why or how these statements are contradictory.

Thus, the record fails to demonstrate defendants' allegedly misleading statements "interfere with the proper administration of a class action, abuse the rights of members of the class," or otherwise require the Court to exercise its discretion to issue an order

pursuant to Rule 23(d). See Dodona I, LLC v. Goldman, Sachs & Co., 300 F.R.D. at 184. Moreover, even if the record showed otherwise, a court may only impose “the narrowest possible relief which would protect the respective parties.” Gulf Oil v. Bernard, 452 U.S. at 102. An order prohibiting all further communications with the putative class members would be overbroad. Id. at 103 (“[A]n order requiring prior judicial approval of all communications, with the exception of cases where respondents chose to assert a constitutional right . . . was an abuse of discretion.”).

Accordingly, based on the present record, the Court concludes an order under Rule 23(d) requiring corrective notice and for a prohibition of defendants’ future communications with putative class members is not warranted.

CONCLUSION

The motion to dismiss the first amended complaint is GRANTED IN PART and DENIED IN PART.

The motion to appoint interim lead class counsel is DENIED.

Plaintiff's motion for an order pursuant to Rule 23(d) is DENIED.

By February 11, 2021, defendants shall file an answer.

By separate Order, the Court will schedule an initial conference. Defendants should be prepared to discuss whether any additional patients have been confirmed to have had their information accessed or viewed, and what, if any, actions defendants have taken to communicate with those patients.

The Clerk is instructed to terminate the motions. (Docs. ##22, 35, 51).

Dated: January 28, 2021
White Plains, NY

SO ORDERED:

A handwritten signature in black ink, appearing to read 'Vincent L. Briccetti', written over a horizontal line.

Vincent L. Briccetti
United States District Judge